Privacy and Data Protection in a User-Centric Business Model for Telecommunications Services

Juan C. Yelmo, José M. del Álamo, and Rubén Trapero

DIT, Universidad Politécnica de Madrid,
Ciudad Universitaria s/n, 28040 Madrid, Spain
{jcyelmo, jmdela, rubentb}@dit.upm.es

Abstract. New business models have come up in different contexts such as the Internet and Telecommunications networks which have been grouped under the umbrella of the buzzword 2.0. They propose the opening up of service platforms in order to increase profits by means of innovative collaboration agreements with third parties. In this paper we go a step further and propose a business model for Telecommunications services where end-users actually become the collaborating third parties. This user-centric business model poses several privacy and data protection concerns that we analyze and for which we propose a solution.

1 Introduction

Many e-companies have been working for a long time just with their own close set of customers and resources. It was one of their treasures and they were reluctant to share them with other companies because they were afraid of losing profits to their competitors. Acting in such a way has lead to walled-garden business models. Their main drawback is that a huge engineering effort has to be spent both on development and marketing in order to get a new service up and running to the market.

On the other hand, new paradigms have arisen in different contexts such as the Internet and Telecommunications, which have been grouped under the umbrella of the buzzword 2.0: Web 2.0 [1], Telco 2.0 [2], Mobile Web 2.0 [3], and so on. Some of their common approaches are:

1. *The idea of a platform*; i.e. there is no hard boundary as in the walled-garden models, but rather, a gravitational core around which the business is created.
2. *Harnessing collective intelligence*; i.e. turn your customers and providers into a global brain, which could be used to enhance your business.
3. *Data is one of the assets a company owns*; notice that most of the time this information is about the company's customers.

Regarding the first point, there is nowadays a trend in Telecommunications and Internet domains towards partnership and the need to build technology platforms that enable third party providers to collaborate. Relevant examples of this trend are British Telecommunications (BT) Project Web21C [4] and Amazon Web Services [5]

Please use the following format when citing this chapter:

Yelmo, J.C., del Álamo, J.M. and Trapero, R., 2008, in IFIP International Federation for Information Processing, Volume 262; The Future of Identity in the Information Society; Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci; (Boston: Springer), pp. 447–461.

platforms, which allow external developers and businesses to build their own applications with a set of Web Services interfaces.

The most innovative case though, is the so called user-centric platform [6]. It allows users (not necessarily technically skilled) to create their own contents and applications (*mashups*) from the combination (composition) of different sources. There are currently few initiatives in user-centric platforms: on the Internet we can find Yahoo Pipes [7], and in the Telecommunications domain we can find the Open Platform for User-centric service Creation and Execution (OPUCE) [8].

User-centric environments support the fast development and supply of innovative services and this provides benefits for the different actors involved:

- The platform provider obtains some profit from the use of its own services and a percentage for the services created by end-users.
- End-users can create their own personalized services that fit their needs better.

Nonetheless, the combination of user-centric environments with social networks allows users to share their services within a community which will promote the most interesting ones at a minimum cost (viral marketing[1]), thus eliminating the main disadvantage of walled-garden business models i.e. development and marketing expenses.

The obvious question now is why should any end-user use my platform rather than someone else's? The answer points to the third idea of the 2.0 approach: data is one of the main assets of a company.

Companies have been collecting information about their customers which has been kept in information silos just for their own use. However, they can now use this information to boost their platforms and take advantage of the benefits the user-centric approaches provide, thus leveraging new and profitable business models. Moreover, in most cases they have even established a trust relationship with their customers, which may be also used as a powerful asset. Nonetheless, customers can also benefit from the use of their identity information with features such as personalization, customization, improved usability, better user experience and enhanced security.

On the other hand, in most countries there are laws which require companies to ensure security and privacy when revealing personal information about a customer, such as the 2002/58/EC [9] and the 95/46/EC [10] Directives, both of the European Union. Thus, we have arrived at a point where we could create open platforms that end-users would use to develop and consume innovative and profitable services as far as their privacy and identity information are protected.

This paper analyses the requirements with regard to privacy and data protection for a user-centric service creation and execution business model. In order to do so, a business model supporting user-centric service creation and execution is first proposed. Then the requirements for privacy and data protection for the business

[1] Viral marketing refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness, through self-replicating viral processes, analogous to the spread of pathological and computer viruses. It can be word-of-mouth delivered or enhanced by the network effects of the Internet. [Source: Wikipedia].

model are analysed, and a solution is proposed. Finally, a case study where these ideas are applied is described.

2 Business models in user-centric service creation and execution environments

The Telecommunication Information Networking Architecture Consortium (TINA-C) states [11] that *a business model defines the different parties involved in service provisioning and their relationships*. In this section we first describe the requirements for a business model to support user-centric service creation and execution. Then we introduce existing business models for Telecommunications and analyze them regarding these requirements. Finally, we present the proposed business model, the participating entities and their relationships.

2.1 Requirements for the business models to support user-centric service creation and execution

End-user service execution – The first requirement is that end-user service execution should be allowed.

End-user service creation – The next requirement is that the business model should support end-user service creation. This will allow end-users to compose their own services from the set of services that is already offered within the platform.

End-user service provision – The business model should allow extensions to accommodate new players in the service provision. Once end-users create new services, they will probably want to provide them to other end-users.

End-user service recommendation – Finally, the business model should allow users to recommend services to other users. This will contribute to the success of a set of high value services from among the great amount of services that are to be created within the platform. These frequently recommended, high value services will actually provide added value to users, and might turn out to become a kind of killer services [12].

2.2 Existing Telecommunications business models

The following three approaches are currently being studied by telecoms operators in order to find the most appropriate business model for the service provision.

Walled garden – Business models for Telecommunications companies (telcos) have traditionally followed the *walled garden* paradigm [13]. The goal has always consisted of subscribers getting everything they wish (services and contents) in the operator's portfolio. Access to outer services is not allowed and third party service providers, if any, appear under the operator's brand name. The user experience is limited to choosing a service and paying for it under different billing plans. All

revenues go directly to the telco from its customers. In this business model end-user service recommendation does not exist at all, since only the operator's selected services are offered to users following operator's criteria.

Bit pipe **–** The bit-pipe approach [14] describes the operator network as bit pipes that allow its customers to access services with neither constrains nor added value. The operator gets its revenue from the use of the network. Users may choose from the set of services offered by third parties. They pay for the services following the service provider terms and conditions, which may differ from provider to provider. The quality of service (QoS) is not checked by the operator, and thus not ensured. The management of identity information and the privacy and data protection is up to each service. Operators do not provide any mechanism to promote or recommend services, since they are not offered by them. In some cases, the third party providers include tools in their services to recommend them to other users (i.e. inviting friends by sending an e-mail with the recommendation). In any case end-user service recommendation may be performed, but out of the scope of the business model.

Semi-walled garden **–** Within this business model customers stay inside the operator's *walled garden* but they are free to choose and enjoy third party services and contents [15]. The revenue is divided between the operator and the provider. Operators offer value-added service enablers that are attractive to third party providers thus encouraging the partnership between them: some are related to the Telecommunications infrastructure (e.g. QoS, SMS service or setting up calls), and other to users' identity (e.g. authentication, presence, location or address books). The network operator, the service provider and content provider, all work together in a team to build a value chain that produces services which may be interesting to the end users and providing some revenue to each member in the chain. Similar to the walled garden case, it is the operator itself who carries out the service recommendation by suggesting as trusted and directly accessible from the service menu those services which belong to selected third parties. The order in which services are prompted to the users determines the actual service recommendation. This order is usually based on off-line agreements between the operator and the corresponding service providers.

The three business models are analyzed in **Table 1** with respect to the proposed requirements.

Table 1. Analysis of Telecommunications business models.

Requirement	***Walled garden***	***Bit pipe***	***Semi-walled garden***
End-user service execution	Yes	Yes	Yes
End-user service creation	No	No	No
End-user service provision	No	No	No
End-user service recommendation	No	Yes (externally)	No

None of the main business models for Telecommunications satisfy the requirements related to end-user service creation and provision. The best approach, the *semi-walled garden,* lets third parties to take part in the business by developing services that the customer could use within the framework provided by the *walled garden*, and that is a first step on the right path. However, the process to become a third party is long and tedious and is not feasible for end-users. Nevertheless, an evolution of the business model is needed which will make it possible also for

customers to create, share and recommend their own services. This is the particularity of the business model we present; the fact that the customer performs now other roles in the business model apart from the service consumer.

2.3 A business model for user-centric service creation and execution

To begin with the description of the proposed business model we present the entities that participate: the operator and the customer. The operator provides the user-centric platform where end-users create and execute their services. It may also provide some services with basic functionality e.g. send an SMS, set up a call, retrieve a presence status or a location, and so forth. Customers may execute the services available, but also create their own. Some third party service providers might also participate, providing specialized contents or services on the operator's platform. In this case their relationship with the operator may be modelled using the semi-walled garden business model. In order to simplify our description we will not consider third party service providers.

The relationships between the different entities and their roles in the user-centric business model are detailed in the following figure.

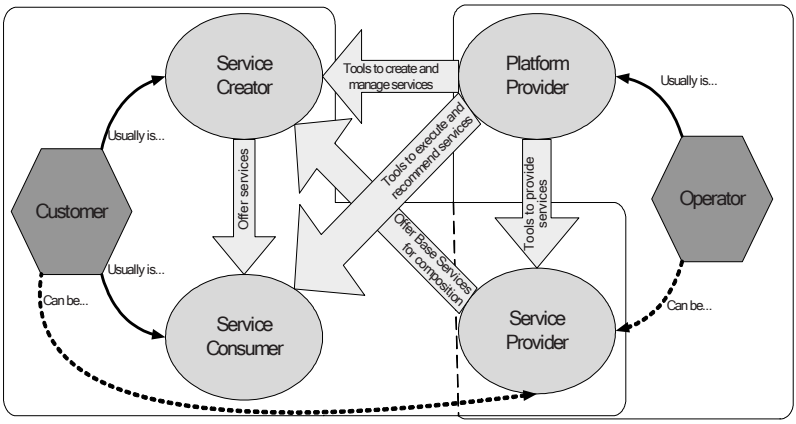

Fig. 1: Entities and roles involved in a user-centric business models.

The roles played by the different entities are: platform provider, service consumer, service creator and service provider. The customer may play the role of service consumer, service creator and service provider. The difference between service creator and service provider is that the former offers services to consumers, while the latter offers its services to other service creators for combination. The operator usually plays the role of platform provider, but as we said it could also provide its own service portfolio for combination thus becoming a service provider too.

The platform provider supplies all the features that enable the creation, the management, the provision, the execution and the recommendation of services. It is also involved in the economic flows between the different members (creators, providers and consumers).

Service creators find that a service is needed and useful (for themselves or for any other member of the community) and have the necessary skills and tools to create it from the set of services already available within the platform. Once the service is created and deployed on the platform it will be available to be used by other service consumers under different billing plans. Successful services may also be used as base services in further compositions, thus becoming service providers too.

To identify which value is perceived by the different actors, we define the value chain of the business. The actors that add value in this value chain are the operator that provides the platform, and the customer that creates services that can be provided. There are no intermediaries between the service creator and the service consumer, except the platform. Therefore the traditional value chain for service provisioning has been shortened to put creators in touch with consumers via a simplified channel (Fig. 2). This new channel should have the means and the tools to simplify both the creation and the consumption of new services.

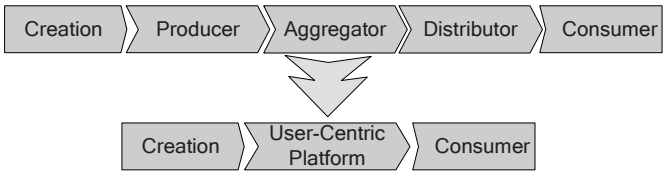

Fig. 2: Value chain for the proposed business model.

Some of the benefits of the business model for different roles are briefly described below:

Customer value **–** The two main factors for the value perceived by the customer are the level of personalization of the services (very personalized since service creators are usually the final users themselves) and later, the chance of sharing them, making the platform a hugely connected network based on user-generated services. The services provided are valuable to all the users belonging to the community as long as they can be personalized more than just because of their own usefulness. In that sense, identity attributes such as age, gender, location or presence status are commonly used for personalization purposes.

Platform value **–** Traditional network businesses base their value on the number of participants that take advantages of their features. A user-centric platform is a network business as well, and thus it is important for its success to have as many members as possible. This will allow the flow of services being shared between service creators and service consumers to increase.

Figure 3 shows the flows of revenue between different roles. The consumer pays the platform (if needed this will be applicable only for premium services) for the use of one final service under different billing plans (monthly fee, pay per use, etc). It could be determined by means of the nature of the service. The service creator receives part of this revenue, which can be proportional to the number of users of their services (this is a revenue-sharing model, but their might be others depending on the service itself). Service providers perceive their revenues from the platform, for example by agreements on percentages for each mashup they are part of. If users perceive the service as valuable, the platform provider and the service creator receive

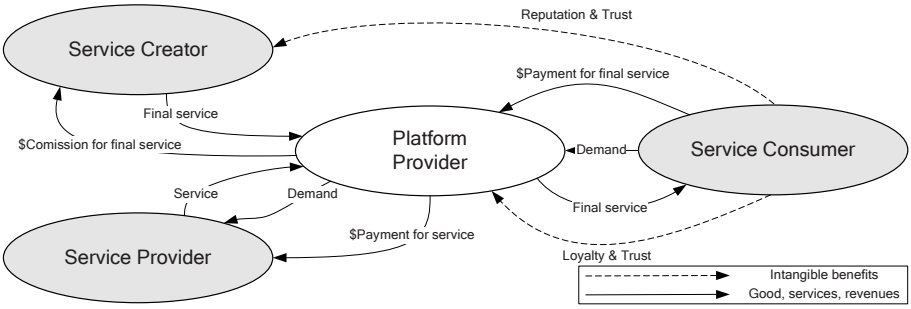

Fig. 3: Flows of revenue for the proposed business model.

intangible benefits such as customer loyalty (the former), reputation (the latter) or trust (both).

3 Privacy issues in the proposed business model

Proper management of identity information provides better usability and improves the user experience, which may be used to enhance user-centric service creation and execution platforms. It is also at the core of the relationship of the platform provider with its customers, both creators and consumers, and other companies such as the service providers; i.e. identity management is a must when enabling access to identity attributes. Moreover, it increases efficiency, enhancing security and open new revenue opportunities. Thus, the use of customers' identity information provides benefits for all the roles in the business model. Some examples are:

- Automated access to the service portfolio supported by single sign-on and dynamic service discovery and invocation, which enhances the usability of the platform and the consumers' user-experience.
- Service adaptability and context awareness, which allows services to react according to the circumstances under which they operate to offer better usability. These circumstances are usually based on consumers' identity attributes such as location, presence status or consumer's device.
- Service personalization, which allows service creators to customize pre-existing services and components based on personal attributes and user profiles.

The next section describes the specific requirements for the business model regarding privacy and data protection issues in terms of their legal and technical approaches. It also proposes a solution to fulfil these requirements.

3.1 Requirements

Proper identity management is essential in every new Telecommunications service that is implemented or provided in Europe. Furthermore, it is obligatory because of restrictions and legal constraints derived from several European Directives:

- European Union Data Protection Directive [16];
- European Union Electronic Communications Privacy Directive [9];
- European Union Data Retention Directive [10].

Within the Data Protection Directive, *personal data* is defined as information that relates to an identified or identifiable natural person. The *processing of personal data* is defined as any operation or set of operations that is performed on personal data, such as collecting, storing, disseminating, and so on. The different dimensions of data protection are:

1. Personal data must be collected for ***specified, explicit and legitimate purposes*** and not further processed in a way incompatible with those purposes.
2. Personal data must be ***adequate, relevant and not excessive in relation to the purposes*** for which they are collected and/or further processed. This can be seen as part of the privacy principle of data minimization, which can be seen in two ways:
    - Avoid that private date might appear scattered in multiple places in the network.
    - Ensure that a unique unit of private data is provided to a certain requester, and not a set of it which may include more private information that the one that is needed.
3. Personal data may be processed only if the data subject has ***unambiguously given her or his consent***.

In the proposed business model there are three roles which may process personal data, and thus may be affected by the Privacy and Data Protection Directives. The platform provider stores consumers' accounts and preferences so it is clear that it processes personal data. Service providers may provide personal information to service creators or use it for different purposes. Service creators may need to use service providers to fulfill some specialized task and thus they might need to provide identity information about the service consumers in order to compose new services.

Taking into account the Data Protection Directive, we can derive the specific requirements for each role:

1. The platform must explicitly state in a **privacy policy** the **purposes** of the personal data it processes. Service providers and service creators must also explicitly state in a privacy policy the purpose of the data it processes. We do not discard to include mechanisms to enforce the fulfillment of such policies, for instance, by using specific alternatives such as the Enterprise Privacy Authorization Language (EPAL) [17].
2. The platform must not release and the service providers/creators must not collect attributes that are irrelevant for the service in question. A special case is that when a service is not interested in the consumers' attributes but on their

authorization to access the service. In this case the platform should derive the authorization from the consumer's attributes without releasing any of them. In any other case the service provider must **explicitly specify the attributes that is processing**.

3. The platform must **ask for consumer consent** for the set of attributes it is processing. Each service must also ask for **consumer** consent for the set of attributes it is processing. When asking for **consumer** consent, the privacy policy that states the purpose and the relevance of the attributes must be available. Furthermore, the user must also be informed about which is the entity that is requesting the attributes (as it is stated in the Article 10 of [10]).
4. Consumers must be allowed to **query the set of identity attributes** the platform has got about them, and to **correct them** when they are not accurate. They must also be able to know which services are using their identity attributes, and **revoke consent** as desired.

The Directives also allocate compliance responsibilities according to the role that any given participant is performing. In that sense liability issues must be taken into account. Therefore:

5. The platform should provide a **liability disclaimer** to prevent misuse and abuses by service creators, service providers and service consumers. Service providers and service creators should also provide liability disclaimers for the use of their services.

3.2 Technical approach to fulfil the privacy and data protection requirements

As we have shown, the platform and the service provider are the roles directly affected by the privacy and data protection directives as they must implement privacy policies that state the identity attributes they use and reason for using them. They should also include liability requirements to prevent misuse and avoid abuses. These requirements are quite straightforward and they could be fulfilled beforehand. On the other hand, the requirements for the service creators must be automatically fulfilled by the tools supporting the creation process.

The approach we propose to fulfill the requirements is:

1. **Privacy policy**. Each service must have a privacy policy that states the identity attributes it uses and reason for using them.
2. **Privacy policy composition**. When a new service is created the policies of the individual components must be automatically aggregated in order to create a new privacy policy that states both the identity attributes it is processing and the purpose. The set of attributes the components are processing must be automatically aggregated and explicitly specified in the new privacy policy (following a concatenation approach for individual privacy policies).
3. **Dynamic management of customers' consent**. The previous point stated that the privacy policy for the new services will contain the set of identity attributes they are using. Thus, at runtime it is possible for the execution environment to retrieve this information, check whether the customer has

granted the service to use her personal information and, if not, explicitly ask her for consent previously to the service execution.

4. **Self management of identity attributes and consents**. As the platform knows from the privacy policies which attributes are being used, by which services and whether it is agreed by the customers or not, then it is feasible to present this information to the customers and allow them to modify it.
5. **Liability disclaims**. Each service must provide a liability disclaimer that disclaims responsibilities resulting from service misuse or abuse. This could be automatically provided by the platform.

To sum up, the platform must enforce each service having a privacy policy, must provide the means to draw up the privacy policies for the new services, and the means to ask consumers for explicit consent on the use of their attributes (at least in the first use of the service). It also must ensure that each service has a liability disclaimer. It is possible to have a unique liability disclaimer for all the services offered on the platform.

4 Case study: OPUCE

The OPUCE project is a research project within the European Union Sixth Framework Programme for Research and Technological Development. OPUCE aims to bridge advances in networking, communication and information technology services towards a unique service environment where personalized services are dynamically created and provisioned by the end-users themselves.

The general objective of OPUCE is to leverage the creation of a user-centric service ecosystem giving users the chance to create their own personalized services as is currently done on the Internet. Within this approach, service concepts are redefined. In OPUCE, services are envisaged as short-lived telecom services that end-users will create by orchestrating simpler services called base services. Base services are considered as functional units deployed by the operator, available on the OPUCE platform and offered to end users through Web Services interfaces.

Figure 4 introduces a detailed diagram of the OPUCE architecture. Its main elements are:

- A *Service Creation Environment* with a set of tools to be used by people or third parties to create services dynamically. It can be seen as a portal through which users can create, manage and share services. Actually, it consists of two portals: a user portal, to manage social networks, service subscriptions and configurations, etc; and a service portal, to manage the service edition, test, simulation, monitoring, etc. The Service Creation Environment also includes other general functions (access control, registration) and administration tools.
- A *Context Awareness* module to manage the adaptation and customization of services to the users' ambience conditions. In OPUCE two types of context aware adaptations are supported: explicit, when it is the service creator who specifies the service behaviour by taking into account user context information; and implicit, when the platform itself analyzes the service and adapts the execution dynamically.

- A *User Information Management* module to control the user's personal information (agenda, buddy list, presence information, device capabilities, potential use of certain services, etc.), identity management and AAA.
- A *Subscription Management* module to keep control of the user subscriptions to services. The information that this module stores is mainly consumed by other OPUCE modules (such as the context awareness or the user information modules).
- A *Service Lifecycle Manager* module which manages the lifecycle of all services created within the OPUCE platform.
- A *Service Execution Environment* which manages the execution of services and orchestrates base services following the logic created by the users when composing them.

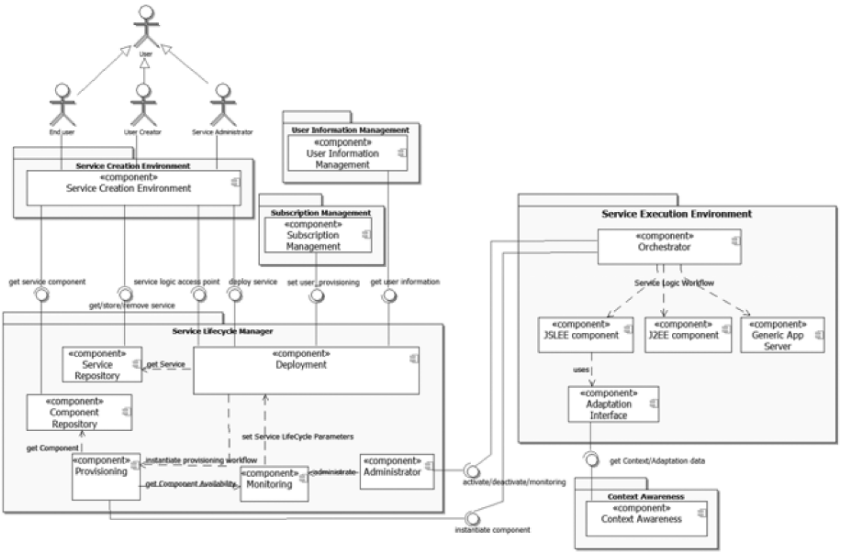

Fig. 4: The OPUCE architecture.

4.1 Privacy requirements fulfilment in OPUCE

A user-centric based service ecosystem requires major flexibility and dynamism in managing privacy and data protection compared to current service management systems. In order to automate the process between the creation and the execution of the services, the OPUCE platform needs a common way to describe the services completely. Therefore services are described using a service specification which contains all aspects of a service. Each aspect, called a facet, is further described in a separate XML-based specification [18] (Figure 5).

Up until now OPUCE has three sets of facets: functional facets include service logic, service interface, service semantic, etc; non-functional facets include service level agreements, quality of service, etc; and management facets include service lifecycle schedule, deployment and provisioning.

Facets are automatically generated and managed by the platform, without service creators taking further action except composing their services. For example, service creators use the Web visual editor to compose their services by orchestrating some of the available ones; the creation process is easy as they have to put together graphical building blocks representing the services they want to use. Then, the platform creates a service logic facet which contains the Business Process Execution Language (BPEL) [19] from the service orchestration. When the creation process has finished the service logic facet is stored in a repository. At the time of deployment, a service lifecycle management module moves the facet into a BPEL engine, where it is ready for execution. For further details on the service lifecycle management refer to [20].

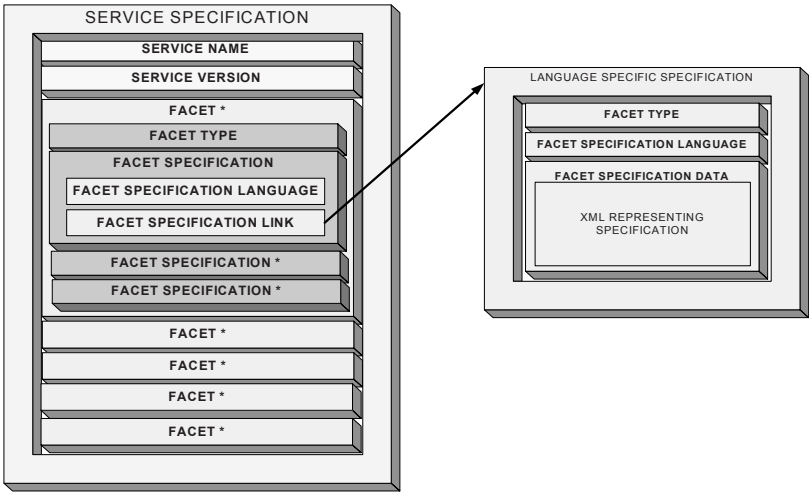

Fig. 5: Service description using a faceted approach.

A requirement derived from the privacy and data protection analysis for a user-centric environment business model is that each service must have a privacy policy. In that sense we see that a fundamental part of a service description is its privacy policy. Therefore a new facet is created: ***privacy policy facet***. This facet contains the privacy policy for the service which includes the set of identity attributes it is processing and the purpose. When a new service is created, a privacy policy facet is created by concatenating individual privacy policy of each base service.

In OPUCE each facet is described in a separate XML-based specification. This allows us to choose any XML-based language to express the privacy policy for the service as far as it complies with our requirements. The Platform for Privacy Preferences (P3P) [21] is a protocol developed by the World Wide Web Consortium (W3C) which defines an XML-based language through which services can describe their privacy policies in a machine readable format. Categories of information include different types of data being collected, the purpose(s) for collection, and which organizations will have access to the collected data. It covers enough of our requirements regarding privacy policies.

As for privacy policy composition, privacy policy facet for the composed services can be created in a similar way as the service logic facet is created i.e. at the time of

creation it is made up of the privacy policy facets of the component services. The new facet is then stored in the repository.

At the time of subscription, the subscription management module would retrieve the privacy policy for the service and prompt users for consent on the use of their identity attributes. It must also ask the consumers for their acceptance of the liability disclaimer. The user information management is the module where this information is stored. At runtime, the service execution environment will check against the user information whether a user has given consent for a service to retrieve identity information. This allows OPUCE to fulfill the requirements regarding dynamic management of customers consent and liability disclaims.

Finally, customers can use the user portal to manage which personal information is being used by which services, and thus revoke consent as desired. Therefore, the last requirement can be fulfilled.

5 Conclusions

User-centric service creation and execution is becoming a new paradigm in the area of Telecommunications service provisioning. It poses several challenges resulting from the short lifecycles of the user-created services as well as the end-users' privacy and data protection in such a dynamic environment.

In this paper we have stated some of the basic requirements for a business model to support user-centric service creation and execution. The main business models in Telecommunications have been analyzed in the light of these requirements. As none of them fulfils the requirements we have proposed a new one describing the parties involved, their roles and their relationships.

For the proposed business model an analysis has been made regarding the privacy and data protection requirements in the European Union. In order to fulfil these requirements we have proposed a set of technical solutions based on the composition of individual privacy policies.

To demonstrate the feasibility of the proposed approaches, we have chosen a user-centric service creation and execution platform for Telecommunications which is currently under development. We have described the specific architecture of the solution and the processes that must take place. The final solution is based on the creation of XML-based service descriptions which include a facet that contains the privacy policy that applies to the service. Regarding service creation, whenever an end-user creates a new service its privacy policy will be generated automatically from the components' privacy policies. This privacy policy will be used at the time of subscription to get the end-users consent for the use of their identity attributes. Eventually, this information will be checked at the execution of the service to ensure privacy and data protection. Further work will tackle the improvement of the user interface for obtaining consents, with explicit mechanisms to inform the user about the privacy policy that will be applied, and asking for acceptance of the terms of the agreement.

Acknowledgements

This work is framed within the IST European Integrated Project OPUCE (*Open Platform for User-centric service Creation and Execution*), 6th Framework Programme, Contract No. 34101. We thank all our partners in the project for their valuable comments and proposals aiming at improving the conceptual model.

References

1. O'Reilly, T.: What is Web 2.0 - Design patterns and business models for the next generation of software. O'Reilly Media Inc, (Sep. 2005); http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html
2. STL Partners Ltd., Telco 2.0 Manifesto: How to make money in an IP-based world (May 2007); http://www.telco2.net/manifesto/
3. Jaokar, A. and Fish, T.: Mobile Web 2.0 (Futuretext, London, 2006)
4. Web21C SDK Developer Center (2007); http://sdk.bt.com/
5. Amazon Web Services (2007); http://www.amazon.com/
6. Caetano, J. et al, Introducing the user to the service creation world: concepts for user centric creation, personalization and notification. International Workshop on User centricity – state of the art. Budapest, Hungary (2007).
7. Yahoo Pipes Website (2007); http://pipes.yahoo.com/pipes.
8. OPUCE Website (2007); http://www.opuce.eu/.
9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201, 37-47 (July 2002)
10. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, Oct. 1995, pp. 31-50.
11. TINA-C Deliverable: TINA Business Model and Reference Points. Version 4.0. (1997)
12. Anderson, C.: The Long Tail: Why the Future of Business is Selling Less of More (Hyperion, New York, 2006)
13. Afuah, A., Tucci, C., Internet Business Models and Strategies (McGraw Hill, Irwin, 2001)
14. Cuevas, A., Moreno, J., Vidales, P., Einsiedler, H.: The IMS Service Platform - A Solution for Next-Generation Networks Operators to Be More than Bit Pipes. IEEE Communications Magazine, vol. 44, no. 8, Aug. 2006, pp. 75-81.
15. Baker, G. and Megler, V., The semi-walled garden: Japan's i-mode phenomenon (IBM pSeries Solutions Development, October 2001).
16. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC, Official Journal L 105, Mar. 2006, pp. 54-63.
17. Powers, C. and Schunter, M. (Ed.): Enterprise Privacy Authorization Language (EPAL 1.2). Version 1.2. IBM Research Report (2003)
18. Sawyer, P., Hutchison, J., Walkerdine, J. and Sommerville, I.: Faceted Service Specification. Proceedings of Workshop on Service-Oriented Computing Requirements (SOCCER'05). Paris, France (2005).
19. Andrews, T. et al, Business Process Execution Language for Web Services. V. 1.1. (2003)

20. Yelmo, J.C., Trapero, R., Del Álamo, J.M., Sienel, J., Drewniok, M., Ordás, I., and McCallum, K.: User-driven service lifecycle management: Adopting Internet paradigms in telecom services. Prpceeding of the International Conference on Service Oriented Computing (ICSOC 2007), Vienna, Austria (2007)
21. W3C Recommendation: The Platform for Privacy Preferences (P3P). Version 1.0. (2002)